release notes

HP StorageWorks Director

Product Version: FW 06.02.00/HAFM SW 08.02.00

Sixth Edition (September 2004)

Part Number: AA–RTDVF–TE/958–000276–006

These release notes contain late-breaking and supplemental information for the HP StorageWorks Director 2/64 and Director 2/140.

For the latest version of these release notes and other director documentation, access the following HP storage web site: http://www.hp.com/country/us/eng/prodserv/storage.html.

Printed in the U.S.A.

HP StorageWorks Director release notes
Sixth Edition (September 2004)
Part Number: AA–RTDVF–TE/958–000276–006

About this document

These release notes contain late breaking and supplemental information for the Director 2/64 and Director 2/140.

Be sure to read these release notes before installing a Director 2/64 and Director 2/140. This information is periodically updated and available on the following HP web site: http://www.hp.com/country/us/eng/prodserv/storage.html.

This section describes the content reflected in this document, including:

Release notes information

These release notes cover the following major topics:

■ SNMP issues, page 22

Intended audience

This document is intended for customers who purchased the Director 2/64 or Director 2/140.

Firmware version 06.02.00-22

Firmware 06.02.00-22 is the latest (as of this date), firmware released with the Director 2/64 and Director 2/140. A copy of firmware 06.02.00-22, is contained on the HP StorageWorks director documentation and firmware CD (Part Number 524-000002-005). The latest firmware is also available on the following HP web site:
http://h18006.www1.hp.com/storage/saninfrastructure.html.

For more information on upgrading firmware versions, refer to the appropriate HP StorageWorks director service manual. The features of this firmware version are detailed in the following manuals.

Other director documentation

In addition to these release notes, HP provides the following corresponding information:

- *HP StorageWorks Director Element Manager Licensing Instructions*, AA-RVHAA-TE/958-000282-000
- *HP StorageWorks Director Torque Tool Caution Flyer*, AA-RTDEC-TE/958-000282-002
- *HP StorageWorks Director Power Cord Advisory*, AA-RTDMC-TE/958-000279-002
- *HP StorageWorks Universal Port Module Kit Installation Instructions*, AA-RSS2D-TE/958-000281-002
- *HP StorageWorks Director 2/140 Installation Guide*, AA-RTDSC-TE/958-000275-002
- *HP StorageWorks Director 2/140 Service Manual*, AA-RTDTC-TE
- *HP StorageWorks Director Element Manager User Guide*, AA-RTDUC-TE
- *HP StorageWorks Director 2/64 Installation Guide*, AA-RSNGD-TE/958-000289-002

- *HP StorageWorks Director 2/64 Service Manual*, AA-RS2ED-TE
- *HP StorageWorks M-Series Rack Mount Kit Installation Instructions*, AA-RQZPE-TE/958-000292-002
- *HP StorageWorks CLI Reference Guide for Directors and Edge Switches*, AA-RQ7AE-TE
- *HP StorageWorks SNMP Reference Guide for Directors and Edge Switches*, AA-RQ7BE-TE
- *HP StorageWorks SAN High Availability Planning Guide*, AA-RS2DD-TE
- *HP StorageWorks SAN Design Guide*, AA-RMPNN-TE
- *HP StorageWorks Embedded Web Server User Guide*, AA-RTDRC-TE
- *HP StorageWorks HA-Fabric Manager User Guide*, AA-RS2CE-TE
- *HP StorageWorks HA-Fabric Manager Transition Guide*, AA-RV1MA-TE
- *HP StorageWorks HA-Fabric Manager Appliance Installation Guide*, AA-RU5FB-TE/958-000324-001
- *HP StorageWorks HA-Fabric Manager Release Notes*, AA-RUR6C-TE/958-000288-007
- *HP StorageWorks Director and Edge Switch Glossary*, AA-RU5JB-TE
- *HP StorageWorks C-FCSWAPI SDK Bridge Agent Installation Instructions*, AA-RVJ1A-TE/958-000405-000

CD-ROM directory structure

The HP StorageWorks director documentation and firmware CD contains the following items:

- `Manuals.pdf`—HP StorageWorks Director 2/64 and Director 2/140 Documentation; links to the following documents and search function
- Documents
  - `README.TXT`—HP document structure; late-breaking doc changes
  - AA-RTDSC-TE/958-000275-002—*HP StorageWorks Director 2/140 Installation Guide*
  - AA-RTDTC-TE—*HP StorageWorks Director 2/140 Service Manual*
  - AA-RTDUC-TE—*HP StorageWorks Director Element Manager User Guide*

  - AA-RSNGD-TE/958-000289-002—*HP StorageWorks Director 2/64 Installation Guide*
  - AA-RS2ED-TE—*HP StorageWorks Director 2/64 Service Manual*
  - AA-RQ7AE-TE—*HP StorageWorks CLI Reference Guide for Directors and Edge Switches*
  - AA-RQ7BE-TE—*HP StorageWorks SNMP Reference Guide for Directors and Edge Switches*
  - AA-RS2DD-TE—*HP StorageWorks SAN High Availability Planning Guide*
  - AA-RMPNN-TE—*HP StorageWorks SAN Design Guide*
  - AA-RTDRC-TE—*HP StorageWorks Embedded Web Server User Guide*
  - AA-RU5FB-TE/958-000324-001—*HP StorageWorks HA-Fabric Manager Appliance Installation Guide*
  - AA-RS2CE-TE—*HP StorageWorks HA-Fabric Manager User Guide*
  - AA-RV1MA-TE—*HP StorageWorks HA-Fabric Manager Transition Guide*
  - AA-RU5JB-TE—*HP StorageWorks Director and Edge Switch Glossary*
  - AA-RVJ1A-TE/958-000405-000—*HP StorageWorks C-FCSWAPI SDK Bridge Agent Installation Instructions*
- Firmware
  - `HPQ_MSF_v06.02.00-22.bin`—HP StorageWorks M-Series firmware
  - `firmwareupdate.txt`—Instructions for updating firmware
- Acrobat
  - `RP505ENU.EXE`—Windows installation file for Acrobat Reader 5.0 with Search

Supported configurations

Operation of multiple switches in a fabric topology is subject to the following topology limits. Consider the impact of these limits when planning the fabric.

Note: For more information about planning the fabric, refer to *HP StorageWorks SAN High Availability Planning Guide*.

- **Fabric Elements**—Each fabric element is defined by a unique domain ID that ranges between 1 and 31; therefore, the theoretical limit of interconnected directors in a single fabric is 31. The supported limit of interconnected switches in a single fabric is 24. Because this number is subject to change, contact your HP authorized service representative for the current number of interconnected switches supported in a single fabric.
- **Inhomogeneous fabric**—To determine if interoperability is supported for a product, or if restrictions apply, refer to the product publications, or contact your HP authorized service representative.
- **Number of Interswitch Links (ISLs)**—The maximum supported number of ISLs is 75% of installed ports for the Director 2/64, and 50% of installed ports for the Director 2/140. For redundancy, at least two ISLs should connect any two director-class fabric elements. Because this number is subject to change, contact your HP authorized service representative for the current number of ISLs supported per director.
- **Hop Count**—The Fibre Channel theoretical limit of ISL connections traversed (hop count) in a single path through a fabric is seven. The maximum supported hop count in a single path through a fabric is three. Because this number is subject to change, contact your HP authorized service representative for the current hop count supported by a single fabric path.

Note: The hop count is equal to the number of ISL connections traversed in a single path, not the total number of ISL connections between devices.

Cable requirements

Note: Optical cables for the Director 2/64 and Director 2/140 must be ordered separately.

For cables measuring up to 500 meters (1 Gbps) or 300 meters (2 Gbps), use multi-mode Fibre Channel cables. For longer cables, use single-mode Fibre Channel cables.

Multi-mode optical cables are connected to short-wave optical transceiver modules in a switch. Single-mode optical cables are connected to long-wave optical transceiver modules in a switch. Multi-mode cables should use 50/125 optical fibers, and single-mode cables typically use 9/125 optical fibers for distances up to 10 km.

Verify that connectors interfacing with the Director 2/64 and Director 2/140 use LC Duplex connectors with a PC finish. In addition, the connector at the opposite end of the cable must be of either LC or SC type, depending on the requirements of the connected device.

Important information

This section describes important information related to the Director 2/64 and Director 2/140.

HAFM and firmware compatibility

Table 1 lists the minimum version of HAFM that can run with the various versions of firmware for the directors and edge switches.

Table 1: HAFM and firmware compatibility

Firmware version	HAFM version (minimum)
01.01.02	04.00.01 (HP EFCM)
01.02.02-06	04.01.02-14 (SDCM)
01.03.00-35	04.02.00-40 (HP EFCM)
01.04.00-01	04.02.00-40 (SDCM)
02.00.00-33	06.00.00-45 (HP EFCM)
02.00.02-01	06.00.02-06
04.01.02-04	06.03.01-05

Table 1: HAFM and firmware compatibility (Continued)

Firmware version	HAFM version (minimum)
05.02.00-13	07.01.00-09 (Notebook Server)
05.02.00-13	07.02.00-09 (HAFM Appliance)
05.05.00-12	None (Edge Switch 2/12)
06.01.00-18	07.01.00-09 (Notebook Server)
06.01.00-18	07.02.00-09 (HAFM Appliance)
06.01.00-18	08.02.00 recommended (HAFM Appliance)
06.02.00-22	07.01.00-09 (Notebook Server)
06.02.00-22	07.02.00-09 (HAFM Appliance)
06.02.00-22	08.02.00 recommended (HAFM Appliance)

Prerequisites for installing and using firmware 06.02.00

If you are using HAFM, firmware 06.02.00 requires HAFM 07.01.00 or later (check with HP Customer Support for the latest shipping version of HAFM). HAFM should be at the minimum level before installing the new firmware.

Note: HAFM is not required for operating hardware products using the firmware.

All directors and edge switches in the same fabric should have the same firmware level installed. Although products may co-exist in a fabric running different levels of firmware, all products *must* be at the same major functional release level.

Upgrading from an earlier version of firmware

Upgrading to firmware 06.02.00-22 is non-disruptive to attached devices. The director or edge switch is not required to be offline before performing an upgrade operation. Limitations to upgrades are clearly identified if there are any limitations to performing the operation.

Before upgrading firmware, it is highly recommended that you back up the director or edge switch configuration. Refer to your *HP StorageWorks Director Element Manager User Guide* for more information. Embedded Web Server (EWS) also provides an option to print or save product configuration to a file. Refer to the *HP StorageWorks Embedded Web Server User Guide* for more information.

All products must be running firmware 05.00.00 or later before upgrading to 06.02.00-22. If a switch is operating with a firmware level earlier than 05.00.00, you must upgrade to 05.xx.xx before installing 06.02.00-22.

Upgrades and downgrades are supported only from one major release to the next, such as from 05.xx.xx to 06.02.00-22. If EWS is used for upgrades and downgrades, and this rule is not followed, errors occur and there may be a disruption to attached devices.

If upgrading to firmware 06.02.00-22 requires you to upgrade from 04.xx.xx to 05.xx.xx in the process, there are special considerations, as detailed in the section, "Upgrading firmware on a director from 04.xx.xx to 05.xx.xx" on page 11.

A small number of early-shipped Surestore Director FC-64 units may receive one of the following messages when they upgrade to firmware 05.02.00-13:

- HAFM—`Firmware cannot be loaded due to insufficient CTP memory.`
- EWS—`File System Error: Insufficient memory for new firmware version.`

This occurs only in certain units with CTP cards. Units with CTP2 cards do not have this issue.

If you get one of these messages during the upgrade, the firmware upgrade failed, but the unit continues working with the existing firmware without an interruption in service. The upgrade process checks for sufficient memory before activating the new firmware image. The firmware upgrade does not complete without sufficient memory. Please contact HP Customer Support if you receive this message.

Upgrading firmware on a director from 04.xx.xx to 05.xx.xx

An issue has been identified in release 04.xx.xx if the contents of the nonvolatile storage (NVRAM) on the active CTP become corrupted. Once the configuration has been loaded, this corruption is not detected until an IPL/IML, power cycle, or firmware code load. If the NVRAM in the active CTP has corrupted contents, the firmware load can cause the configuration to reset to factory defaults, which could cause a system outage. By using the following procedure to upgrade firmware, configuration is preserved and a system outage is avoided. This issue was corrected with firmware 05.02.00-13 and later.

Note: Step 4 of the following procedure is not required if you are upgrading from 05.xx.xx or later.

To safely upgrade firmware on a director, perform the following:

1. Upgrade HAFM software on the HAFM server/appliance to 07.01.00 (minimum).
2. Download firmware 05.02.00-13 using the **Firmware Library** option under the Product Manager Maintenance menu.
3. Back up the director configuration using the **Backup & Restore Configuration** option under the Product Manager Maintenance menu.
4. Using the Product Manager, execute a CTP swap:

Note: You must have maintenance authorization rights to access the HAFM Product/Element Manager menu options used in this procedure.

---

   a. From Product/Element Manager Hardware view, verify that an amber LED indicator is not displayed for either CTP card.
   b. Right-click the CTP card you believe to be active. From the right-click pop-up menu, choose **FRU Properties**. Verify that it is the active CTP card.
   c. Right-click the active CTP card and choose **Switchover** from the pop-up menu.

Note: The director loses its Ethernet connection for a short period during the switchover process.

When switchover occurs, the green LED illuminates on the backup CTP card to indicate that it is now the active card.

5. Upgrade the firmware to 05.02.00-13 on each director using the **Send** option on the Firmware Library dialog box.

Considerations for downgrading the version of firmware

Directors or edge switches are not required to be offline before performing a firmware downgrade operation. Limitations to downgrades are clearly identified if there are any limitations to performing the operation.

Before downgrading firmware, it is highly recommended that you back up the director or edge switch configuration. Refer to your *HP StorageWorks Director Element Manager User Guide* for more information. EWS also provides an option to print or save product configuration to a file. Refer to your *HP StorageWorks Embedded Web Server User Guide* for more information.

Downgrading directly to a release before 05.00.00 from 06.02.00-22 is not allowed. To downgrade to a release before 05.00.00, you must first downgrade to 05.YY.ZZ.

Upgrades and downgrades are supported only from one major release to the next, such as from 05.xx.xx to 06.02.00-22. If EWS is used for upgrades and downgrades, and this rule is not followed, errors occur and there may be a disruption to attached devices.

Note: The Director 2/140 and the Edge Switch 2/24 cannot be downgraded earlier than 04.01.00, and the Edge Switch 2/12 cannot be downgraded earlier than 05.05.00.

If a Director 2/140 in a multiswitch fabric is downgraded earlier than 06.02.00, ISLs could become segmented if there are any other switches in the fabric operating with an firmware version earlier than 06.01.00. To prevent this situation, downgrade all Director 2/140s in the fabric to 06.01.00 before downgrading any products in the fabric to 05.xx.xx. This problem only exists with Director 2/140s in the fabric. HAFM displays a warning message if a downgrade from 06.02.00 is attempted, but you can continue with the downgrade if desired.

Note: The warning message is displayed when downgrading any model from 06.02.00, but only applies to downgrade operations for the Director 2/140.

Firmware downgrades should not be performed using EWS and Internet Explorer v5.00.3315.1000x. If this operation is performed, the download operation may not complete and may eventually time-out leaving the switch with the previous version of firmware.

HAFM upgrade required for firmware version 06.xx.xx

To upgrade to firmware 06.xx.xx, you must first upgrade the HAFM software to 07.01.00-9 minimum, if you are using the notebook HAFM server to manage the director or edge switch. The HAFM software is contained on the HP StorageWorks ha-fabric manager documentation and software CD (Part Number 516-000024-820). An upgrade kit to HAFM 07.01.00-9 is also available, Part Number 320908-B22, for owners of license for previous versions. This HAFM upgrade is also available on the following HP web site: http://h18006.www1.hp.com/storage/saninfrastructure.html.

If you are using the 1U rack-mount HAFM appliance to manage the director or edge switch, the minimum HAFM version required is 07.02.00-9, which is the minimum version installed. This HAFM software is contained on the HP StorageWorks ha-fabric manager documentation and software CD (Part Number 516-000024-720).

The previous minimum versions of HAFM allow you to manage directors or edge switches running 06.02.00-22 firmware, but to be able to use all the new features and enhancements, you need to upgrade HAFM to 08.02.00, which runs only on the 1U rack-mount HAFM appliance. The next major firmware release requires the use of an HAFM version, which runs only on the HAFM appliance.

As an alternative, you can perform the firmware upgrade directly to the director or edge switch using their EWS.

Please contact your local HP technical resource if you need to obtain a new HAFM version.

Please contact your local HP technical resource to confirm compatibility with devices in your SAN before upgrading to this firmware version.

For more information on upgrading software versions, refer to the *HP StorageWorks HA-Fabric Manager User Guide.* The features of this software version are detailed in the accompanying manuals listed in section "Other director documentation" on page 4.

OSMS change

Open Systems Management Server (OSMS) is now available as a standard feature. OSMS can be enabled/disabled via EWS, Command Line Interface (CLI), and HAFM.

Default zone is disabled by default

The default zone on the Director 2/64 and the Director 2/140 is disabled by default. Zoning must be configured in order for any devices connected to the director to communicate.

Some IP addresses must be avoided

If you use HAFM to manage other M-Series Fabric directors and edge switches, when you select IP addresses for edge switches, directors, and for the HAFM appliance, do not use IP addresses in the following range:

192.168.0.0 through 192.168.0.255—This subnet is used internally to the HAFM appliance. Using an IP address in this range causes the call-home feature to function incorrectly.

Hard zoning

Hard zoning is a security enhancement introduced in firmware 05.01.00-24 that prevents ports from accessing devices outside their zones. Hard zoning is enabled by default when using firmware 05.01.00-24 or greater and cannot be disabled. All HP-approved host bus adapters (HBAs) limit access to devices within their zones, so you will not see a change in fabric behavior unless you are using nonstandard HBAs. Hard zoning improves security against intruders that load nonstandard HBA drivers.

Hard zoning is compatible with legacy zone definitions, including World Wide Name (WWN) and port zoning. You can use your existing zones and zone sets without any changes. There are no changes to the zoning interfaces, so you do not need to modify your zone management practice, modify your documentation, or retrain Storage Area Network (SAN) administrators.

Hard zoning controls access at the ingress port. When a port attempts to send a frame to a destination outside its zones, the frame is blocked. A Class 2 frame is fabric rejected, and a Class 3 frame is dropped.

Zoning change RSCN control

Normally, when a zone set is activated, a fabric format domain Register State Change Notification (RSCN) is sent to all devices in the fabric. With firmware 05.00.00 or later, you can disable these RSCNs from being sent. This is done using the **Suppress RSCNs on zone set activations** check box on the Configure Switch Parameters dialog box.

This feature significantly changes the normal behavior of the fabric. Devices will have no warning when zones change and will not automatically update their zoning information. The ability to suppress RSCNs is disabled (check box is not selected) by default. This feature can be configured through HAFM, EWS, and CLI.

SNMP changes

Firmware 06.02.00-22 supports the following management information base (MIB) versions on all products:

- Fabric Element MIB: 1.1
- MIB-II MIB: RFC-1213, non-implemented sections are not included
- FCEOS MIB: 2.0
- SNMP Framework MIB: RFC-2271 (1997/09/30)
- FA MIB: 3.0
- FA MIB: 3.1

SNMP requests can be received in either 3.0 or 3.1 of the Fibre Alliance (FA) MIB, and the switch responds in the same version. The switch can also be configured to use a specific version for traps generated by the switch.

Zoning limitations

With firmware 06.00.00 and later, you have the ability to configure large zone sets, including up to 1024 zones and 1024 end ports in a single zone set. Table 2 shows the supported limits for the edge switches and directors.

Table 2: Zoning parameters supported limits

Zoning parameter	Maximum value
Number of zone members in a zone	2048
Number of zones in a zone set	1024
Number of unique zone members in a zone set	2048
Total number of zone members in a zone set (where a zone member can be in multiple zones)	4096
Characters per zoning name	32
Number of unique zone members in HAFM Zoning Library	2048
Number of zones in HAFM Zoning Library	1024
Number of zone sets in HAFM Zoning Library	64
Number of end ports	1024
Number of devices supported (including loop devices)	1024

Using the same firmware

All directors and edge switches in the same fabric should have the same firmware level installed—whether 1 Gbps or 2 Gbps capable, this firmware operates correctly.

The recently released Edge Switch 2/12 had an interim firmware specific for the Edge Switch 2/12, 05.05.00-12. This firmware cannot be used for any other edge switch or director. This interim version is compatible with the M-Series firmware 05.01.00-24 and 05.02.00-13 used for the rest of the M-Series fabric products. The firmware 06.02.00-22 is a common firmware for all the M-Series fabric products, including the Edge Switch 2/12.

Firmware 06.02.00-22 includes minor bug fixes, and provides support for second-generation Edge Switch 2/12 and Edge Switch 2/24 switches. This is the minimum M-Series firmware supported on the second-generation Edge Switch 2/12 and Edge Switch 2/24.

For customers who want to add a second-generation switch to their existing SAN, but are not ready to upgrade their SAN from 5.x to 06.02.00, there is a downgrade firmware version for each of these edge switches which provides compatibility with a SAN running 05.02.00.

Firmware 05.03.01-01 is available for the Edge Switch 2/24, and firmware 05.05.01-01 is available for the Edge Switch 2/12. These versions are installed only on the Edge Switch 2/24 and Edge Switch 2/12, and only when these switches are placed in a M-Series SAN running 05.02.00 firmware. A copy of these versions of firmware, are contained on the HP StorageWorks edge switch documentation and firmware CD (Part Number 524-000001-005).

Reinstalling feature licenses

Feature licenses (or keys) must be reinstalled after performing a factory reset on a director to regain use of the licensed features (e.g., SANtegrity Binding).

Disconnecting the null modem cable

Always log out and disconnect the null modem cable from the serial maintenance port when not in use or when the switch is reset.

CTP controls port lights

Port lights on the edge switch and director products are controlled by the CTP functionality. Certain activities such as firmware updates, IPLing the CTP, or switching over to the backup CTP (director) can cause these port lights to extinguish momentarily until control is reasserted by the CTP. The actual Fibre Channel traffic is not affected during these times.

Ethernet switch support

With firmware 06.00.00 and later, customers can now connect the management port on edge switches and directors to Ethernet switches or hubs. Prior to firmware 06.00.00, only connections to Ethernet hubs were qualified and supported.

Full Volatility

Full Volatility is an optional feature of firmware 06.00.00 and later that is enabled with a feature key. The Full Volatility feature is designed to support high-security environments, which require that customer data not be retained by the edge switch or director after power off.

The feature configures a switch or director so that no frame data is stored after a power off. Without Full Volatility, if the switch or director experiences a fault condition, a dump of the embedded memory space is captured into non-volatile memory. This dump retains the last 30 frames transmitted from and last four frames transmitted to the embedded port. With Full Volatility installed, this dump does not occur when a fault condition occurs. Although this limits the amount of diagnostic information available for potential problem resolution, the vast majority of problems are typically resolved without the dump files.

Contact your sales representative to purchase a feature key for Full Volatility.

CLI threshold alerts

With firmware 06.00.00 and later, the CLI allows you to set and monitor Throughput Threshold Alerts (TTAs).

CLI show.eventLog command

With firmware 06.00.00 and later, the CLI `show.eventLog` command has been enhanced. The command now displays a Link Incident log and Event log.

MIHPTO value

With firmware 06.00.00 and later, the internal Missing Interrupt Handler Primary Time Out (MIHPTO) value has been changed from 15 seconds to 3 minutes.

Route management—Preferred Path

Preferred Path can be configured using either CLI or HAFM 08.02.00.

Preferred Path allows you to influence the route of data traffic when it traverses multiple switches or directors in a fabric. If more than one interswitch link (ISL) connects switches in a fabric, you can specify an ISL preference for a particular flow. The data path consists of the source port of the switch or director being configured, the exit port of that switch or director, and the domain ID of the destination switch or director. Each switch or director must be configured for its

part of the desired path to achieve optimal performance. You may need to configure Preferred Paths for all switches or directors along the desired path for proper multi-hop Preferred Path operation.

This feature allows use of the fabric shortest path first (FSPF) for any undefined or erroneous path definitions and uses standard rerouting algorithms when errors in the fabric occur. Thus if the defined route is not valid, the standard, automatically generated route, is used.

When a Preferred Path is defined for all of the ports on a switch, it provides a reasonable level of predictability because it isolates changes in routing only to the ports affected by a particular “preferred path.” Thus, if the “preferred path” goes away, only the ports assigned to the path are rerouted to other paths. Conversely, if the “preferred path” is re-established, the ports assigned to the path are rerouted back to the path.

The Preferred Path enhancement modifies the behavior of Open Trunking by providing guidance for the balancing function. The paths are balanced according to the Open Trunking guidelines after the Preferred Path selections have been assigned. Thus, the Preferred Path selections are eliminated from the list of candidates to be moved off of a flow.

The Preferred Path configuration allows you to assign the exit port assignment, but is subject to the standard rules regarding the FSPF protocol. Thus, if the indicated path is not a least-cost route, the FSPF algorithm takes precedence. Likewise, any port that does not have a Preferred Path definition is subject to the static load-balance rules. And finally, a Preferred Path is not excluded from the FSPF path selection operation for undefined or recovered paths.

Note: Activating a new Preferred Path will cause a reroute to occur if the Preferred Path is different from the current path. In congested environments, with traffic on the current path, a reroute can cause an out-of-order frame (OOOF) at the destination device. Reroutes are a natural activity in any Fibre Channel fabric when the network is modified. For example, reroutes occur when ISLs are added or lost or when new switches are added to the fabric. Fibre Channel devices are designed to handle errors such as OOOFs, but some devices send error messages. In FICON environments, an IFCC error can result from an OOOF. To avoid these error messages, vary devices s offline before a Preferred Path is activated, and then return the devices to online status afterwards.

EWS enhancements

With firmware 06.00.00 and later, EWS enhancements include support for managing the SANtegrity Binding feature and **Enterprise Fabric** mode, and providing the Link Incident log and the Open Trunking log.

Known issues

This section describes the known issues related to the Director 2/64 and Director 2/140.

HSG80 transparent mode not supported with IBM AIX

Use of an HSG80 with IBM AIX is restricted to operating the HSG80 in Multibus mode with the Director 2/64 and Director 2/140. Transparent mode is not supported at this time.

Workaround

None.

HSG80 transparent mode not recommended with controller in SCSI-3 mode with HP-UX operating systems

Due to an issue with non-existent duplicate LUNs being displayed with the HP-UX operating systems, the HSG80 controller is restricted to SCSI-2 mode of operation when set to Transparent failover mode.

SCSI-3 mode of operation in Multibus failover mode is fully supported with the use of Secure Path software, 3.0 or later versions.

Workaround

None.

ISL disconnect causes NOS error with the OpenVMS operating systems

When an ISL connection is physically removed between directors or switches, the Fibre Channel Adapter model FCA2354 transmits a Not Operational Sequence (NOS) error. This is observed as an entry in the HAFM appliance Link Incident log for the port in which the FCA2354 is attached. The director's Hardware View also displays a yellow triangle icon over the port that detected this incident. The fabric operation or data movement is not disrupted by these incidents, and you can clear alerts from these incidences using the following procedure.

Workaround

Use these steps to clear the incident alerts.

1. At the **HAFM Hardware View**, click the port module to open the **Port Card View**.
2. Right-click on the port with the yellow triangle icon, and choose **Clear Link Incident Alert(s)**.

Support for speed Auto-Negotiate

Auto-negotiate is supported. However, HP recommends that the port speed for E_Ports (for Interswitch Links, or ISLs) be set to a specific port speed (**1Gb/sec** or **2Gb/sec**, as appropriate for the speed of the directors or edge switches being connected) instead of to **Negotiate**. Using a specific port speed decreases the time for a fabric build in response to some perturbation event in the fabric. Similarly, setting a specific port speed for N_Ports also decreases fabric build time. However, setting a specific port speed for N_Ports is not required.

There are a few older HBA devices that do not always succeed in logging in to a switch port when the port speed is set for auto-negotiate.

Workaround

If an older HBA has difficulty logging into a switch port that has its port speed configured as **Negotiate**, configure that port speed to **1Gb/sec** or **2Gb/sec** according to the operation speed of the HBA connected to that port.

Ports may accumulate spurious events

A port may accumulate *Invalid transmission word* and *Bit-Error Threshold Link Incident* events when a transceiver is poorly seated, resulting in a poor ground connection.

Workaround

Reseating the optical transceiver corrects the problem.

IML is required after performing a configuration reset

If a **Reset Configuration** is performed on a Director 2/140 to reset the director to factory configuration, you must perform an initial machine load (IML) to complete the process. This is done by pressing the white button on the front of either CTP card for more than three seconds. This can also be accomplished by turning the power to the Director 2/140 off and then back on.

Possible switch reset after power failure or power off sequence

In extremely rare instances, after a power failure or power off sequence, an edge switch or director configuration may be reset to factory default settings. This is evident when HAFM is unable to communicate with the edge switch or director after being powered on. This condition occurs because the IP address assigned to the edge switch or director has been reset to the factory default value (10.1.1.10).

Workaround

If this condition occurs, the configuration of the edge switch or director must be restored, and the IP address must be restored. Also, all licensed features need to be reactivated by entering the license keys again.

Deleting a certain switch binding member using EWS may cause an error

An error `154 Invalid membership list` occurs if you delete the last member on the last page of the Switch Binding Membership List, and then you delete the last member on the first page of the Switch Binding Membership List.

Workaround

Add additional members to the end of the list, and then you delete the intended member.

SNMP issues

SNMP traps `warmStart` and `coldStart` are not always received across Ethernet switches.

Workaround

None.